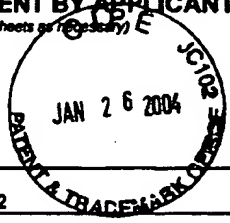


#14

Substitute for form 1449A PTO
**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Use as many sheets as necessary)



Complete if Known	
Application Number	09/541667
Filing Date	March 31, 2000
First Named Inventor	Ellison, Carl
Group Art Unit	Unknown
Examiner Name	Unknown

RECEIVED

JAN 28 2004

Sheet 1 of 2

Attorney Docket No: 42P08629 Technology Center 2100

US PATENT DOCUMENTS

Examiner Initial *	USP Document Number	Publication Date	Name of Patentee or Applicant of cited Document	Class	Subclass	Filing Date if Appropriate
--------------------	---------------------	------------------	---	-------	----------	----------------------------

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Foreign Document No	Publication Date	Name of Patentee or Applicant of cited Document	Class	Subclass	T*
m	DE-4217444	12/03/1992	Toyohisa, Imada, et al.	G06F	12/08	
m	EP-0473913	03/11/1992	Farrell, Joel A.	G06F	9/46	
m	JP-2000076139	03/14/2000	Tanno, Masaaki, et al.	G06F	12/11	
m	WO-0175564	10/11/2002	Herbert, Howard C., et al.	G06F	1/00	
m	WO-02086684	10/31/2002	Proudlar, Graeme J.	G06F	1/00	
m	WO-0217555	02/28/2002	Ford, Warwick	H04L	19/08	

No English Translation

OTHER DOCUMENTS -- NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No*	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T*
m		BRANDS, STEFAN, "Restrictive Blinding of Secret-Key Certificates", SPRINGER-VERLAG XP002201306, (1995), Chapter 3	
m		CHIEN, ANDREW A., et al., "Safe and Protected Execution for the Morph/AMRM Reconfigurable Processor", 7th Annual IEEE Symposium, FCCM '99 Proceedings, XP010359180, ISBN 0-7695-0375-6, Los Alamitos, CA, (4/21/1999), 209-221	
m		COMPAQ COMPUTER CORPORATION, et al., "Trusted Computing Platform Alliance (TCPA) Main Specification Version 1.1a", (12/2001), 1-321	
m		DAVIDA, GEORGE I., et al., "Defending Systems Against Viruses through Cryptographic Authentication", Proceedings of the Symposium on Security and Privacy, IEEE Comp. Soc. Press, ISBN 0-8186-1939-2, (May 1989),	
m		IBM, "Information Display Technique for a Terminate Stay Resident Program IBM Technical Disclosure Bulletin", TDB-ACC-No. NA9112156, Vol. 34, Issue 7A, (12/1/1991), 156-158	
m		KARGER, PAUL A., et al., "A VMM Security Kernel for the VAX Architecture", Proceedings of the Symposium on Research in Security and Privacy, XP010020182, ISBN 0-8186-2060-9, Boxborough, MA, (5/7/1990), 2-19	
m	B:	KASHIWAGI, KAZUHIKO, et al., "Design and Implementation of Dynamically Reconstructing System Software", Software Engineering Conference, Proceedings 1996 Asia-Pacific Seoul, South Korea 4-7 Dec. 1996, Los Alamitos, CA USA, IEEE Comput. Soc. US, ISBN 0-8186-7638-8, (1996),	
m		LUKE, JAHN, et al., "Replacement Strategy for Aging Avionics Computers", IEEE AES Systems Magazine, XP002190614, (March 1999),	
m		MENEZES, OORSCHOT, "Handbook of Applied Cryptography", CRC Press LLC, USA XP002201307, (1997), 475	
m		RICHT, STEFAN, et al., "In-Circuit-Emulator Wird Echtzeitauglich", Elektronik,	

EXAMINER

m

DATE CONSIDERED

2/25/04

Substitute for Form 1449/PTO (Modified)

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)



Complete if Known

Application Number	09/541,667
Filing Date	March 31, 2000
First Named Inventor:	Carl M. Ellison
Group Art Unit	2787
Examiner Name	Unassigned
Attorney Docket Number	042390P8629

RECEIVED
NOV 25 2002
Technology Center 210

Sheet	2	of	2
-------	---	----	---

OTHER ART - NO PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T ²
		GOLDBERG, R., "Survey of virtual machine research," IEEE Computer Magazine 7(6), pp. 34-45, 1974.	
		GUM, P.H., "System/370 Extended Architecture: Facilities for Virtual Machines," IBM J. Research Development, Vol 27, Number 6, pp. 530-544, November 1983	
		ROSENBLUM, M. "Vmware's Virtual Platform: A Virtual Machine Monitor for Commodity PCs," Proceedings of the 11th Hotchips Conference, pp. 185-196, August 1999.	
		LAWTON, K., "Running Multiple Operating Systems Concurrently on an IA32 PC Using Virtualization Techniques," http://www.plex86.org/research/paper.txt ; 11/29/1999; pp. 1-31.	

Examiner Signature		Date Considered	8/25/05
--------------------	---	-----------------	---------

*Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication.

¹Unique citation designation number. ²Applicant is to place a check mark here if English language Translation is attached.









Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.



ELECTRONIC INFORMATION DISCLOSURE STATEMENT

Electronic Version v18

Stylesheet Version v18.0

Title of Invention	Attestation Key Memory Device and Bus						
Application Number:	09/541667						
Confirmation Number:	3630						
First Named Applicant:	Carl Ellison						
Attorney Docket Number:	42P08629						
Art Unit:	Unknown						
Examiner:	Unknown Unknown						
Search string:	(20030018892 or 4162536 or 4247905 or 4276594 or 4307447 or 4347565 or 4759064 or 4795893 or 4825052 or 4907270 or 4907272 or 4910774 or 5007082 or 5139760 or 5317705 or 5319760 or 5434999 or 5437033 or 5442645 or 5504922 or 5511217 or 5522075 or 5528231 or 5533126 or 5566323 or 5606617 or 5720609 or 5721222 or 5737604 or 5796835 or 5825875 or 5854913 or 5867577 or 5900606 or 5901225 or 5903752 or 6061794 or 6075938 or 6092095 or 6182089 or 6212635 or 6222923 or 6269392 or 6272637 or 6308270 or 6314409 or 6330670 or 6363485 or 6374286 or 6374317 or 6378072 or 6397242 or 6412035 or 6421702 or 6435416 or 6445797 or 6463537 or 6557104).pn.						
<div>RECEIVED JAN 28 2004 Technology Center 2100</div>							
US Patent Documents							
Note: Applicant is not required to submit a paper copy of cited US Patent Documents							
init	Cite.No.	Patent No.	Date	Patentee	Kind	Class	Subclass
	1	20030018892	2003-01-23	Tello, Jose		713	164
	2	4162536	1979-07-24	Morley, Richard E.		714	18
	3	4247905	1981-01-27	Yoshida, Yukihiro , et al.		711	166
	4	4276594	1981-06-30	Morley, Richard E.		713	1660
	5	4307447	1981-12-22	Provanzano, Salvatore R., et al.		700	1
	6	4347565	1982-08-31	Kaneda, Saburo , et al.		711	6
	7	4759064	1988-07-19	Chaum,		380	30

2	8	4795893	1989-01-03	Ugon, Michael
2	9	4825052	1989-04-25	Chemin, Francois , et al.
2	10	4907270	1990-03-06	Hazard, Michel
2	11	4907272	1990-03-06	Hazard, Michel
2	12	4910774	1990-03-20	Barakat, Simon
2	13	5007082	1991-04-09	Cummins, Mary T.
2	14	5139760	1994-06-07	Mason, Andrew H., et al.
2	15	5317705	1994-05-31	Gannon, Patrick M., et al.
2	16	5319760	1994-06-07	Mason, Andrew H., et al.
2	17	5434999	1995-07-18	Goire, Christian , et al.
2	18	5437033	1995-07-25	Inoue, Taro , et al.
2	19	5442645	1995-08-15	Ugon, Michel , et al.
2	20	5504922	1996-04-02	Seki, Yukihiro , et al.
2	21	5511217	1996-04-23	Nakajima, Atsushi , et al.
2	22	5522075	1996-05-28	Robinson, Paul T., et al.
2	23	5528231	1996-06-18	Patarin, Jacques
2	24	5533126	1996-07-02	Hazard, Michel , et al.
2	25	5566323	1996-10-15	Ugon, Michel
2	26	5606617	1997-02-25	Brands, Stefanus A.
2	27	5720609	1998-02-24	Pfefferle, William C.
2	28	5721222	1998-02-24	Bernstein, Peter R., et al.
2	29	5737604	1998-04-07	Miller, David A., et al.
2	30	5796835	1998-08-18	Saada, Charles
2	31	5825875	1998-10-20	Ugon, Michel
2	32	5854913	1998-12-29	Goetz, John W., et al.
2	33	5867577	1999-02-02	Patarin, Jacques
2	34	5900606	1999-05-04	Rigal, Vincent
2	35	5901225	1999-05-04	Ireton, Mark A., et al.
2	36	5903752	1999-05-11	Dingwall, Thomas J., et al.
2	37	6061794	2000-05-09	Angelo, Michael E.
2	38	6075938	2000-06-13	Bugnion, Edouard , et al.
2	39	6092095	2000-07-18	Maytal, Benjamin
2	40	6182089	2001-01-30	Ganapathy, Narayanan , et al.
2	41	6212635	2001-04-03	Reardon, David C.
2	42	6222923	2001-04-24	Schwenk, Joerg
2	43	6269392	2001-07-31	Cotichini, Christian , et al.

235 382
 235 380
 713 181
 705 65
 705 181
 705 67
 423 328.1
 718 100
 711 208
 717 167
 714 16
 714 736
 703 25
 718 100
 718 100
 340 5.8
 713 187
 711 154
 380 30
 431 326
 514 89
 713 1
 713 172
 705 65
 712 210
 705 67
 235 375
 714 7
 718 103
 726 3
 703 27
 718 100
 707 206
 713 165
 380 44
 709 200

44	6272637	2001-08-07	Little, Wendell L., et al.	713	194
45	6308270	2001-10-23	Guthery, Scott B., et al.	726	9
46	6314409	2001-11-06	Schneck, Paul B., et al.	705	54
47	6330670	2001-12-11	England, Paul, et al.	713	2
48	6363485	2002-03-26	Adams, Carlisle	713	186
49	6374286	2002-04-16	Gee, John K., et al.	718	108
50	6374317	2002-04-16	Ajanovic, Jasmin, et al.	710	105
51	6378072	2002-04-23	Collins, Thomas, et al.	713	187
52	6397242	2002-05-28	Devine, Scott W., et al.	718	1
53	6412035	2002-06-25	Webber, Victor	710	261
54	6421702	2002-07-16	Gulick, Dale E.	718	102
55	6435416	2002-08-20	Slassi, Tarik	253	492
56	6445797	2002-09-03	McGough, Paul, et al.	380	285
57	6463537	2002-10-08	Tello, Jose A.	713	182
58	6557104	2003-04-29	Vu, Son T., et al.	713	189

Remarks

Note: Remarks are not for responding to an office action.

Applicants, in accordance with their duty of disclosure under 37 CFR 1.56 and in accordance with 37 CFR 1.97(c)(2), hereby submit this Electronic Information Disclosure Statement citing U.S. Patent documents for consideration by the Examiner. Pursuant to 37 CFR 1.97, the submission of this Electronic Information Disclosure Statement is not to be construed as a representation that a search has been made and is not to be construed as an admission that the information cited in this statement is material to patentability. This Electronic Information Disclosure Statement is being filed after the mailing of a first office action and before the mailing of a final office action, notice of allowance, or an action otherwise closing prosecution. Pursuant to 37 CFR 1.97(c)(2), the fee set forth in 37 CFR 1.17(p) of \$180.00 is due for the filing of this Electronic Information Disclosure Statement. Please charge this fee and any other fee that may be due to Deposit Account 02-2666. Applicants respectfully request that the cited documents be considered and that the form be initialed by the Examiner to indicate such consideration and a copy thereof be returned to Applicants' attorney of record.

Signature

Examiner Name	Date
---------------	------